Miao Yu

Research Interests	I work on system security, operating system, virtualization, and formal verification. Specifically, my research mainly focuses on on-demand isolating security-sensitive applications from untrustworthy commodity OSes and applications, protecting sensitive applications' communications with their I/O devices, and verifying these systems.		
CAREER	Project Scientist , Carnegie Mellon University, PA, USA03/2022 Post-doc Researcher , Carnegie Mellon University, PA, USA11/2019	e - Current - 03/2022	
Education	Carnegie Mellon University (CMU), PA, USA8/2012Ph.D. in Electrical and Computer Engineering1Dissertation: An I/O Separation Model and its Applications to On-DemarCommodity PlatformsAdvisor: Virgil D. Gligor	- 11/2019 nd I/O on	
	Shanghai Jiao Tong University (SJTU), Shanghai, China9/200M.S. in Computer Software and Theory9/200Thesis: Vis: Virtualization Enhanced Live Forensics Acquisition for Native Acquisit	5 - 3/2012 3/2012 System	
	B.S. in Software Engineering	7/2009	
Selected Honors and Awards	CMU Innovation Fellows, Ann and Martin McGuinn Graduate Fellowship, Carnegie Institute of Technology Dean's Tuition Fellowship, SJTU Excellent Undergraduate Thesis,	2016 2013 2012 2009	
Books & Chapters	NewBluePill: Hardware Virtual Machine Under the Hood (In Chinese). Miao Yu and Zhengwei Qi. Tsinghua Press, 2011		
Selected Journals	 Dancing with Giants: Wimpy Kernels for On-Demand I/O Isolation. Zongwei Zhou, Miao Yu, and Virgil D Gligor. IEEE Security & Privacy, April, 2015. VGRIS: Virtualized GPU Resource Isolation and Scheduling in Cloud Gaming. Zhengwei Qi, Jianguo Yao, Chao Zhang, Miao Yu, Zhizhou Yang, and Haibing Guan. ACM Transactions on Architecture and Code Optimization (TACO), June, 2014. 		
	vGASA: Adaptive Scheduling Algorithm of Virtualized GPU Resource in Cloud Gaming. Chao Zhang, Jianguo Yao, Zhengwei Qi, Miao Yu, Haibing Guan. IEEE Transactions on Parallel and Distributed Systems (TPDS), November, 2013.		
	Vis: Virtualization Enhanced Live Forensics Acquisition for Native System. Miao Yu, Zhengwei Qi, Qian Lin, Xianming Zhong, Bingyu Li, and Haibing Digital Investigation , May, 2012.	Guan.	
Selected Conferences	An I/O Separation Model for Formal Verification of Kernel Implementations Miao Yu, Virgil D Gligor, and Limin Jia. Proceedings of the IEEE Symposium on Security and Privacy (Oakland), May, 2021.		
	Trusted Display on Untrusted Commodity Platforms. Miao Yu, Virgil D Gligor, and Zongwei Zhou. Proceedings of the ACM SIGSAC Conference on Computer and Communicat rity (CCS), October, 2015.	ions Secu-	

	Dancing with Giants: Wimpy Kernels for On-Demand I/O Isolation. Zongwei Zhou, Miao Yu, and Virgil D Gligor. Proceedings of the IEEE Symposium on Security and Privacy (Oakland), April, 2014	4.
	VGRIS: Virtualized GPU Resource Isolation and Scheduling in Cloud Gaming. Miao Yu, Chao Zhang, Zhengwei Qi, Jianguo Yao, Yin Wang, and Haibing Guan. Proceedings of the International Symposium on High-performance Parallel and Distributed Computing (HPDC), June, 2013.	3-
	Vis: Virtualization Enhanced Live Acquisition for Native System. Miao Yu, Qian Lin, Bingyu Li, Zhengwei Qi, and Haibing Guan. Proceedings of the Second Asia-Pacific Workshop on Systems (APSys), July, 2011.	
	Enhanced Privilege Separation for Commodity Software on Virtualized Platform. Mingyuan Xia, Miao Yu, Qian Lin, Zhengwei Qi, and Haibing Guan. IEEE International Conference on Parallel and Distributed Systems (ICPDS), December, 2010.	1-
Selected Workshops	SPAD: Software Protection Through Anti-Debugging Using Hardware Virtualization. Miao Yu, Mingyuan Xia, Qian Lin, Peijie Yu, Min Zhu, Shang Gao, Zhengwei Qi, Xu Liu, Haibing Guan. XFocus Information Security Conference (XCON), 2011.	le
	HBSP: A Lightweight Hardware Virtualization Based Framework for Transparent Soft ware Protection in Commodity Operating Systems. (In Chinese) Miao Yu, Peijie Yu, Shang Gao, Qian Lin, Min Zhu, and Zhengwei Qi. China National Computer Congress (CNCC), 2009.	t-
Selected Patents	Method and Apparatus for On-Demand Isolated I/O Channels for Secure Applications #10,235,515 - 201 Virgil D Gligor, Zongwei Zhou, and Miao Yu	s. 9
	Method and Apparatus for Trusted Display on Untrusted Computing Platforms to Secur Applications. #10,769,312 - 202 Virgil D Gligor, Zongwei Zhou, and Miao Yu	те 10
	Resource Scheduling System and Method under Graphics Processing Unit Virtualizatio Based on Instant Feedback of Application Effect. #10,922,140 - 202 Miao Yu, Zhengwei Qi, Haibing Guan, and Yin Wang	n
	Accurate Obtaining Memory Content on Running System. #ZL201110190086.5 - 201 Miao Yu, Zhengwei Qi, and Haibing Guan	1
Media Coverage	A Big Step Towards Cybersecurity's Holy Grail. June, 202 Daniel Tkacik	1
	CyLab Research Sheds Light on Heartbleed and Its Implications. April, 201 Richard Power	4